Amendments to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended): A method for validating a user's authorization to run a tool in a service control manager (SCM) module by a security manager, comprising:

obtaining a list of target nodes and a tool definition from a runnable tool, wherein the tool definition specifies roles associated with a tool via an authorization model, and wherein the roles define which management functions a user can perform on target nodes associated with the SCM module;

obtaining ~~the tool's~~ roles associated with a tool from the tool definition;

checking if any of the ~~tool's~~ roles associated with the tool are enabled;

checking if the user is authorized on the target nodes; and

checking if the user is authorized for at least one of the ~~tool's~~ enabled roles on the target nodes.

2. (currently amended): The method of claim 1, wherein the obtaining the ~~tool's~~ roles step includes obtaining the ~~tool's~~ roles associated with the tool, wherein the tool may be assigned one or more roles.

3. (original): The method of claim 1, further comprising validating the roles.

4. (original): The method of claim 1, further comprising obtaining the user's authorized roles for each node in the list of target nodes from a hash table.

5. (original): The method of claim 1, further comprising reporting whether the tool is runnable by the user.

6. (original): The method of claim 5, wherein the reporting step includes reporting the tool as not runnable by the user when all the roles are disabled.

7. (original): The method of claim 5, wherein the reporting step includes reporting the tool as not runnable by the user when the user is not authorized on each of the nodes.

8. (currently amended): The method of claim 5, wherein the reporting step includes reporting the tool as not runnable by the user when the user is not authorized for any of the ~~tool's~~ enabled roles on all of the nodes.

9. (currently amended): A service control manager (SCM) module for validating a user's authorization to run a tool on one or more target nodes, comprising:

target nodes that are managed servers;

tools that specify commands or options on the target nodes, each tool including a tool definition, wherein the tool definition specifies roles associated with a tool via an authorization model;

~~users that manage systems using the tools;~~

~~tools' enabled~~ roles associated with a tool, the roles defining which management functions a user can perform on the target nodes associated with the SCM module ~~that are assigned to users to run the tools~~; and

a security manager that checks whether any of the roles associated with the tool is enabled, and whether the user is authorized for one of the ~~tools'~~ enabled roles.

10. (original): The SCM module of claim 9, wherein the tools are single-system aware (SSA) tools.

11. (original): The SCM module of claim 9, wherein the tools are multi-system aware (MSA) tools.

12. (original): The SCM module of claim 9, wherein the target nodes can be target node groups.

13. (currently amended): A method for validating a user's authorization to run a tool in a service control manager (SCM) module by a security manager, comprising:

obtaining a list of target nodes and tool definition from a runnable tool, wherein the tool definition specifies roles associated with a tool via an authorization model, and wherein the roles define which management functions a user can perform on target nodes associated with the SCM module;

obtaining ~~the tool's~~ roles associated with the tool from the tool definition;

checking if any of the roles associated with the tool are enabled; and

checking if the user is authorized for one of the ~~tool's~~ roles associated with the tool on all of the target nodes, wherein the user assigned with one of the ~~tool's~~ roles on all of the target nodes is authorized to run the tool.

14. (currently amended): The method of claim 13, wherein the obtaining the ~~tool's~~ roles step includes obtaining the ~~tool's~~ roles associated with the tool, wherein the tool may be assigned one or more roles.

15. (original): The method of claim 13, further comprising validating the roles.

16. (original): The method of claim 13, further comprising obtaining the user's authorized roles for each node in the list of target nodes from a hash table.

17. (original): The method of claim 13, further comprising reporting whether the tool is runnable by the user.

18. (original): The method of claim 17, wherein the reporting step includes reporting the tool as not runnable by the user when all the roles are disabled.

19. (original): The method of claim 17, wherein the reporting step includes reporting the tool as not runnable by the user when the user is not authorized on each of the nodes.

20. (currently amended): The method of claim 17, wherein the reporting step includes reporting the tool as not runnable by the user when the user is not authorized for any of the ~~tool's~~ enabled roles on all of the nodes.